In-Class Assignment TBM4: Oracle Manipulation

Digital Finance – BSc Course Prof. Dr. Joerg Osterrieder

Context. A DeFi lending protocol accepts the token MNGO as collateral, valuing it at the spot price reported by a single on-chain DEX oracle. Borrow-LTV = 80%. An attacker already holds \$10M of MNGO (at honest spot). Liquidity in the DEX pool is thin enough that a \$5M buy pumps the MNGO price 5× for several blocks.

Q1. Using the pumped oracle price, compute (a) the attacker's collateral value, (b) the maximum dollar amount they can borrow, and (c) the net profit after the attacker abandons the position (pump cost + original holdings are forfeited).

Solution. (a) Pumped collateral value = \$10M × 5 = \$50M. (b) Max borrow at 80% LTV = 0.80 × \$50M = \$40M. (c) Net profit = \$40M − \$5M (pump cost) − \$10M (original holdings forfeited) = \$25M, ignoring slippage on unwind. This is the Mango Markets (Oct 2022) playbook, where Avraham Eisenberg extracted \$114M in the real event.

Q2. A governance proposal replaces the spot oracle with a 30-minute TWAP (time-weighted average price). In 1–2 sentences, explain why TWAP *reduces but does not eliminate* the attack.

Solution. TWAP averages the pumped price with 30 min of prior honest prices, so the effective over-collateralisation shrinks relative to spot manipulation, but a well-funded attacker can (i) sustain the pump across the full TWAP window or (ii) target a market with thin *baseline* volume so even the 30-min average lifts materially. Longer windows raise the attacker's capital cost but cannot drive the attack probability to zero as long as a single venue dominates price discovery.

Q3. Name *two* post-2022 mitigations that production oracle networks (e.g. Chainlink, Pyth) have actually deployed.

Solution. (1) **Multi-source median / OCR** (Chainlink Off-Chain Reporting): aggregates prices from $\geq$7 independent node operators pulling from $\geq$3 CEX/DEX sources, discarding outliers before publishing. (2) **Deviation circuit breakers**: lending protocols (Aave v3, Compound III) pause liquidations when a single feed diverges $> X\%$ (typically 2–5%) from a cross-feed median. Also acceptable: Pyth confidence intervals (publishes a price $\pm\sigma$ and protocols size positions against the lower bound); staked/slashable oracles (UMA, Chronicle).